SECTION 3: SECURITY

3.1 DSRS SECURITY

In order to use the DSRS for X/Motif, approved users will be assigned an account for the DSRS application. Each account will be assigned a User ID and Password.

This section provides an explanation for security features of the DSRS and highlights the user's responsibilities to ensure the integrity of the DSRS and system assets.

3.1.1 SYSTEM ACCESS CONTROLS

The DSRS access control mechanisms are hardware and software features, operating procedures, management procedures, and various combinations of these designed to detect and prevent unauthorized access and to permit authorized access to the system. There are two major access control mechanisms of the DSRS that are of particular importance to users: identification and authentication mechanisms, and discretionary access control mechanisms.

User Identification and Authentication

The identification and authentication of users is the single most important access control mechanism afforded by the DSRS. The process of identification and authentication defines the identity of the subject (user) that the DSRS Trusted Computing Base (TCB) creates to act on the user's behalf. All subsequent access control decisions depend on this information being correct. The system integrity of the DSRS is based upon the ability to accurately, consistently, and positively identify each user's login session. Otherwise, controlled access protection cannot be assured, and any audit data collected are rendered useless.

Identification and authentication is accomplished by the DSRS and the underlying operating system through the use of an User ID and Password as stated in Section 4.3.

It is imperative that individual accountability be established for DSRS users and, as such, the issuance of a login name and its associated password requires that the user protect the

password from disclosure. The user is further obligated to select a password that is unique and not easily deduced by others.

Some general password selection guidelines follow:

DO NOT

- use your login name in any form (as-is, reversed, capitalized, doubled, etc.).
- use your first, middle, or last name in any form.
- use your spouse's or child's name.
- use other information easily obtained about you.
- use a password of all the same digit or all the same letter.
- use a word contained in English or foreign language dictionaries, spelling lists, or other word lists.
- use a password shorter than six characters.

DO

- use a password with non-alphabetic characters.
- use a password that is easy to remember, so you don't have to write it down.
- use a password that you can type quickly, without having to look at the keyboard.

The unauthorized and knowing disclosure of a password, or use of another individual's login name are both violations of the Computer Fraud and Abuse Act of 1986, Public Law 99-474 and may be punishable under Chapter 47 of Title 18 of the United States Code and under the Uniform Code of Military Justice.

Discretionary Access Control

Discretionary access control is a means of restricting access to objects (RAs) based upon the identity of subjects (users) and/or groups to which they belong. Additionally, these access controls must be capable of including or excluding access to the granularity of a single user. Discretionary access control is provided in the DSRS by the UNIX file system protection bits and the user's group membership within the DSRS application.

File permission in the UNIX operating system is a means of controlling the modes of access that different users have to a UNIX file. Each file has a set of access-mode attributes associated with its i-node entry. These attributes contain read, write, and execute access attributes for each of the three types of user categories: Owner, Group, and Others. Users of the DSRS are restricted to read access for all RAs in the system through the use of file permission bits and are further restricted to specific RAs through the assignment to a specific group within the DSRS.

3.1.2 AUDIT

There is a requirement for the DSRS to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of access to the RAs it protects. The DSRS and the UNIX operating system provide the capability to record, examine, and review security-relevant activities on the system. As previously stated, the integrity of the audit mechanism is highly dependent upon the integrity of the Identification and Authentication mechanism. Unless the system positively identifies users, it cannot correctly associate their actions with them, and no audit mechanism can be effective.

3.1.3 USER SECURITY RESPONSIBILITIES

The security of the DSRS is the responsibility of everyone involved in the use and operation of the system. As a user of the DSRS you share certain general responsibilities for information resource protection. Adherence to the following guidelines should direct your actions when using this Federal computer system:

a. The DSRS is a Federal computer system and, as such, should only be used for lawful and authorized purposes.

b. Once you receive an account on the DSRS, you are personally accountable and responsible for your activity on the system.

c. Do not disclose your password to anyone. The unauthorized and knowing disclosure of a password, or use of another individual's user account, are violations of the Computer Fraud and Abuse Act of 1986, Public Law 99-474 and may be punishable under Chapter 47 of Title 18 of the United States Code and under the Uniform Code of Military Justice. If you suspect that your password has been compromised, change it immediately and contact the DSRS Staff.

d. Never leave your terminal unattended while an active DSRS session has been established. Doing so may result in an unauthorized user gaining access to the DSRS using the account for which you are personally accountable and responsible.

e. The data (RAs) extracted from the DSRS shall be used only for Government, non-commercial or non-profit purposes.

f. Users shall strictly abide by and adhere to any and all restrictive markings placed on the data (RAs), and the user shall not knowingly disclose or release the data (RAs) to third parties who are not engaged in work related to Government, non-commercial, or non-profit purposes.

g. Any restrictive markings on the data (RAs) shall be included on all copies, modifications, and derivative works, or any parts or portions thereof, in any form, manner or substance, which are produced by the user including, but not limited to, incorporation of the data into any other data, technical data, computer software, computer programs, source code, or firmware, or other information of like kind, type or quality. In all such events, the user shall clearly denote where such data initiates and concludes by use of annotations or other such standard markings.

h. Ensure that mechanisms used for the purpose of Identification and Authentication (I&A), such as user identification and passwords, are protected.

i. Use government computer systems only for lawful and authorized purposes.

j. Observe policies and procedures established by the Software Reuse Program (SRP) for the operation of the DSRS.

k. Treat information generated by the DSRS as you would any valuable asset.

l. Recognize that you are accountable for your activities on Government computer systems.